FirstNet needs cyber safeguards

GCN By Kathleen Hickey

March 23, 2015

Public-safety answering points (PSAPs) and other 911 service providers need to hire cybersecurity professionals and have continuity plans in place for cyber disasters, said Bill Schrier, senior policy analyst and First Responder Network Authority (FirstNet) point of contact for the state of Washington and former CTO for the city of Seattle.

In a podcast with IWCE's Urgent Communications, Schrier spoke about security and cybersecurity related to PSAPs and 911systems. The discussion on topics broached at the forum on Cyber & ICT Security for Emergency Calling and Communications, held in early March and hosted by the Industry Council for Emergency-Response Technologies (iCERT).

"It is important to have these discussions now, because if we're going to build a network for public safety, we have to make sure network and device security are primary considerations during the design phase. Not only will building security in at the beginning make security better and more robust, but it also will drive down enterprise cost," said Patrick Flynn, director, Homeland/National Security Programs, Intel Security and chair of the iCERT Cyber & ICT Security Committee in a Medium article discussing the iCert conference.

PSAPs are responsible for answering calls to an emergency telephone number for police, firefighting and ambulance services and dispatching these services. Today most PSAPs have IP-based networks, although they usually are closed networks, with some leading states having ESInet, said Schrier. The Emergency Services IP Network, or ESInet, delivers voice, video, text and data to the PSAP.

" Next Generation 911 (NG911) brings new concerns," said Schrier. One of the bigger ones: citizens can send texts, documents, pictures and videos to a 911 call center that could hold a virus that could affect the call center or first responders.

FirstNet, which will permit multiple agencies and departments to communicate and share data when responding to a single large event, also has security holes.

Established through a 2012 law, the FirstNet network will use technology similar to commercial cell phone networks' 4G broadband service to help connect on-scene data, dashboard cameras, body cameras and other necessary media-linked devices for the best interoperability. Access to 4G will allow for mobile web access, video conferencing and HD video specifically designed for public safety officers and first responders.

While most of the security challenges have been identified, no one has yet come up with solutions, said Schrier.

"One of the issues is identification and access management," he said. A police officer may use an IP-based network to lookup warrants, while an emergency technician may be accessing or generating HIPAA (the federal Health Insurance Portability and Accountability Act, which, protects the confidentiality and security of healthcare information) data, he said. Both may be using the same device.

"How do you make sure the person using the device has the authority to access the data?" he asked. Currently the cellular networks don't have the capabilities to identify the individual using the device.

Another concern is putting sensitive public safety information into the cloud – which has had many high profile breaches.

A roundtable at the forum on securing cloud services believed it was inevitable that PSAP data would move into the cloud. A key to securing this data is the underlying security of cloud technology providers, such as Microsoft and Amazon, which "can hire a lot more people than PSAPs," said Schrier. These cloud technology providers must be compliant with federal, state and local security regulations. A current example: Microsoft performs background checks on employees in its data centers to meet HIPAA regulations and have built its cloud networks to [certain] specifications, he said.

Still, many data breaches in the private sector have occurred at the point of sale at a merchant, not in the cloud, said Schrier. "The parallel in public safety would be individual systems … in

PSAPs or fire departments. The breach might occur when they are disconnected from the cloud," he said.

All these potential problems are reasons why public safety organizations need disaster plans and cybersecurity professionals on staff, Schrier said.

Link to Article

Link to GCN News Articles